T-TRAIL: Preventing Decreased Rank Attacks in RPL-based IoT Networks

Pieter Tolsma
w.e.p.tolsma@student.tudelft.nl

Supervisor: Chhagan Lal
Responsible Professor: Mauro Conti

1. Introduction

- Internet of Things rapidly expanding.
- Need for **efficient** and **secure** routing.
- Routing Protocol for Low Power And Lossy Networks (RPL) proposed in 2012.

- The **Rank Attack** forms a threat to RPL (Fig. 1) by disrupting topology and controlling traffic flow.
- Succesfully **mitigating** the rank attack depends on the **network configuration** and **method** used.

- Research question: *"What effect does the use of a **nonlinear objective function** have on existing mitigation solutions for the **rank attack** on RPL and how can possible exploits be **defended against**?"*

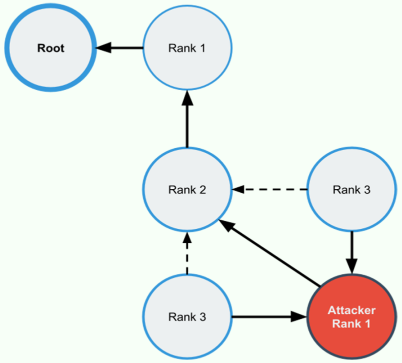

Fig. 1: Decreased Rank Attack

2. Contribution

- **Analyze** well-cited mitigation solutions and expose weaknesses.
- Propose an **improvement** to mitigate found weaknesses.
- Compare **overhead** of proposal to **existing solutions**.

3. Objective Functions and their Security Risks

- Objective function controls the rank increase in RPL network.
- **Nonlinear objective function (NOF)**: rank-increase is nonlinear.
- Using NOF opens up **possibilities** for decreased rank attack but **improves** energy-efficiency.
- Most mitigation proposals do not mention the effects of NOFs.

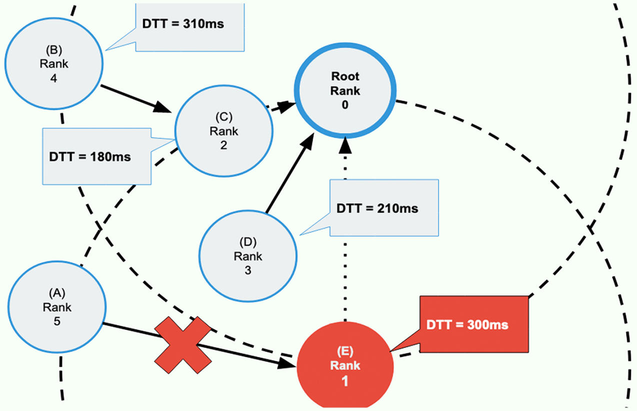

Fig. 2: Outlier Detection using T-TRAIL

4. T-TRAIL

- TRAILs [1] challenge-response mechanism allows round-trip path validation.
- Timed-TRAIL is an extension of TRAIL.
- Measures **Downward-Trip-Time (DTT)** to detect **outliers**.
- Root transmits **signed timestamp**.
- **Probabilistic** method to detect increased rank attack for when NOF is used.

5. Effect of T-TRAIL

- T-TRAIL adds **computational overhead** and increases **convergence time**.
- When NOF is used, T-TRAIL could offer **better protection** than other mitigation solutions.

6. Future Work

The proposed DTT metric can be used in **detection schemes** for a broad range of attacks. Further research is needed in **simulating** T-TRAIL to discover the effectiveness.

References

[1] H. Perrey, M. Landsmann, O. Ugus, M. W ahlisch, and T. C.Schmidt, "Trail: Topology authentication in rpl," in Proceedings of the 2016 International Conference on Embedded Wireless Systems and Networks, ser. EWSN '16.USA:Junction Publishing, 2016, p. 59–64